

Application No. 10826814 (Docket: CNTR.2226)
37 CFR 1.111 Amendment dated 01/10/2008
Reply to Office Action of 09/28/2007

RECEIVED
CENTRAL FAX CENTER
JAN 10 2008

AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus in a microprocessor is provided for accomplishing cryptographic operations. The apparatus includes a cryptographic instruction, CBC block pointer logic, and execution logic. The cryptographic instruction is received by a computing device/microprocessor as part of an instruction flow executing on the microprocessor/computing device. The cryptographic instruction prescribes one of the cryptographic operations. The one of the cryptographic operations includes a plurality of CBC block cryptographic operations performed on a corresponding plurality of input text blocks. The CBC block pointer logic is operatively coupled to the cryptographic instruction. The CBC block pointer logic directs the computing device to update pointer registers and intermediate results for each of the plurality of CBC block cryptographic operations. The execution logic is operatively coupled to the CBC block pointer logic. The execution logic executes the one of the cryptographic operations.

[0022] One aspect of the present invention contemplates a apparatus for performing cryptographic operations. The apparatus includes a cryptography unit within a device/disposed within a microprocessor, and CBC block pointer logic. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes the one of the cryptographic operations. The one of the cryptographic operations includes a plurality of CBC block cryptographic operations performed on a corresponding plurality of input text blocks. The CBC block pointer logic is operatively coupled to the cryptography unit. The CBC block pointer logic directs the device/microprocessor to update pointer registers and intermediate results for each of the plurality of CBC block cryptographic operations.

Application No. 10826814 (Docket: CNTR.2226)
37 CFR 1.111 Amendment dated 01/10/2008
Reply to Office Action of 09/28/2007

[0023] Another aspect of the present invention comprehends a method for performing cryptographic operations in a device. The method includes via a cryptography unit within a microprocessor, executing one of the cryptographic operations responsive to receiving a cryptographic instruction, wherein the cryptographic instruction prescribes the one of the cryptographic operations. The executing includes performing a plurality of CBC mode block operations on a corresponding plurality of input text blocks. The method also includes writing a current input text block to an initialization vector location so that a following one of the plurality of CBC mode block operations on a following one of the plurality of input text blocks will employ the current input text block as an initialization vector equivalent.